Homeland Security

Daily Open Source Infrastructure Report
16 December 2015

Top Stories

- The U.S. Navy announced December 14 that its littoral combat ship, the USS Milwaukee, broke down December 10 due to a loss of propulsion days after the ship's crew discovered fine metal debris in the port combining gear filter system. – *CNN* (See item **4**)

- The U.S. Department of Justice announced that a U.S. Army National Guard soldier pleaded guilty December 14 to collaborating with a co-conspirator to provide material support to ISIL. – *U.S. Department of Justice* (See item **22**)

- MacKeeper, the utility software for Apple Mac products, reported that its database containing passwords and the personal information of 13 million users were exposed in a data breach. – *Help Net Security* (See item **23**)

- The West Linn Police Department arrested 6 adults and 1 minor November 29 for allegations that the suspects were linked to a theft ring scheme in which they victimized 110 people across 7 States by using stolen credit cards to purchase thousands of gift cards. – *The Oregonian* (See item **27**)

Fast Jump Menu

Energy Sector

1. *December 14, Dayton Daily News* – (Ohio) **Identity theft devices found on gas pumps in 7th Ohio county.** Authorities in Ohio found skimming devices on gas pumps in Warren County December 10, bringing the total number of State counties affected to seven. State and local authorities are investigating an organized Cuban crime ring believed to be tied to the installation of the devices in Ohio, Michigan, Illinois, Indiana, Wisconsin, and Kentucky.
Source: http://www.mydaytondailynews.com/news/news/crime-law/identity-theft-devices-found-on-gas-pumps-in-7th-o/npjrH/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *December 15, NBC News* – (New York) **Nuclear reactor at New York's Indian Point is shut down.** Entergy Corp. officials reported that its Indian Point nuclear power plant located in New York was shut down for an undetermined amount of time December 14 following an electrical disturbance that was related to a high voltage transmission line carrying electricity from its Unit 3 nuclear reactor to an offsite electrical switch yard. Authorities stated there was no threat to the public and no radioactivity was released.
Source: http://www.nbcnews.com/news/us-news/nuclear-reactor-new-yorks-indian-point-shut-down-n480146

Critical Manufacturing Sector

3. *December 15, U.S. Consumer Product Safety Commission* – (National) **Kawasaki expands recall of Teryx and Teryx4 recreational off-highway vehicles due to injury hazard.** Kawasaki Motors Corp., issued a nationwide recall December 15 for around 19,500 of its model years 2012 – 2013 Teryx4 750, model years 2014 – 2016 Teryx 800 4x4, and model years 2014 – 2016 Teryx 4 800 recreational off-highway vehicles following 628 incident reports of debris cracking or breaking through the floor boards which resulted in 8 injuries.
Source: http://www.cpsc.gov/en/Recalls/Recall-Alerts/2016/Kawasaki-Expands-Recall-of-Teryx-and-Teryx4-Recreational-Off-Highway-Vehicles/

Defense Industrial Base Sector

4. *December 14, CNN* – (National) **New $360 million Navy ship breaks down.** The U.S. Navy announced December 14 that its littoral combat ship, the USS Milwaukee, broke down December 10 due to a loss of propulsion days after the ship's crew discovered fine metal debris in the port combining gear filter system. The ship needed to be towed more than forty miles to undergo a full inspection in Little Creek, Virginia.
Source: http://www.cnn.com/2015/12/14/politics/uss-milwaukee-breaks-down/index.html

Financial Services Sector

5. *December 15, Softpedia* – (National) **Two mobile banking trojans used Facebook Parse as C&C server.** Security researchers in Germany announced that the Android/OpFake and Android/Marry banking trojans targeting mobile devices stored their command and control (C&C) servers on 5 Facebook Parse databases, the company's BaaS (Backend-as-a-Service) offering, and gathered nearly 170,000 short message service (SMS) messages from infected devices in addition to successfully executing over 20,000 commands primarily for financial fraud. Facebook closed all five accounts in August.
   Source: http://news.softpedia.com/news/two-mobile-banking-trojans-used-facebook-parse-as-c-c-server-497597.shtml

6. *December 15, Newark Star-Ledger* – (New Jersey) **Woman pleads guilty to $1.1 million Securities and Annuities fraud scheme.** New Jersey State officials announced December 14 that a former Morris County investor pleaded guilty December 11 to orchestrating a 10-year, $1.178 million Securities and Annuities fraud scheme by fabricating more than 100 financial statements to inflate her 14 clients' accounts, stealing money from client accounts, fraudulently using the logos of at least 9 corporations, and collecting unlawful financial adviser fees after her license was revoked.
   Source:
   http://www.nj.com/somerset/index.ssf/2015/12/woman_pleads_guilty_to_11_million_securities_and_a.html

For additional stories, see items **1** and **27**

Transportation Systems Sector

7. *December 14, St. Helens Chronicle* – (Oregon) **Truck, rail car accident closes Hwy 30 in St. Johns.** Highway 30 near St. Johns Bridge in Portland was shut down for several hours December 13 while first responders cleared the scene of a fatal 2-vehicle crash involving a semi-truck and immobile rail tankers that killed 1 person.
   Source: http://www.thechronicleonline.com/news/truck-rail-car-accident-closes-hwy-in-st-johns/article_dbb392ce-a29e-11e5-a435-b3b3af376caf.html

8. *December 14, Federal Aviation Administration* – (National) **FAA announces small UAS registration rule.** The U.S. Federal Aviation Administration announced December 14 a new streamlined web-based aircraft registration process will be implemented for owners of small unmanned aircrafts (UAS) that weigh more than 0.55 pounds and less than 55 pounds including payloads such as on-board cameras. The registration is a statutory requirement that applies to all aircrafts to help users operate their unmanned aircraft safely.
   Source: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856

9. *December14, Inland Empire Press Enterprise* – (California) **San Bernardino: I-215S**

big-rig crash causes sigalert, lengthy cleanup. Officials closed 3 southbound lanes of Interstate 215 in San Bernardino for approximately 5 hours while officials worked to clear the wreckage from a 2-vehicle crash that spilled fuel onto the roadway.
Source: http://www.pe.com/articles/bernardino-789340-san-crash.html

10. *December 14, KGET 17 Bakersfield*– (California) **Bomb squad reports suspicious package at Bakersfield Amtrak station was not explosive.** The Amtrak station in Bakersfield was closed and all rail traffic was stopped in both directions December 14 while the Bakersfield Police Department bomb squad and HAZMAT crews investigated a suspicious package found at the station. Officials deemed the area safe and reported the package was not an explosive.
Source: http://www.kerngoldenempire.com/news/police-investigating-suspicious-package-at-bakersfield-amtrak-station

11. *December 14, WHIO 7 Dayton* – (Ohio) **Crash cleared, U.S. 35 West in Dayton reopens.** U.S. 35 West in Dayton was shut down for approximately 3 hours December 14 while officials worked to clear the wreckage from a multi-vehicle crash that caused several injuries.
Source: http://www.whio.com/news/news/local/multiple-vehicle-crash-shuts-35-west-in-dayton/npjq6/

12. *December 13, unionoracle.com* – (Florida) **Fatal crash ties up traffic on SB I-75 in Pasco County.** Southbound lanes of Interstate 75 in Pasco County were closed for approximately 6 hours December 13 while officials investigated the scene of a fatal multi-vehicle crash that killed 1 driver.
Source: http://unionoracle.com/12790-fatal-crash-ties-up-traffic-on-sb-i-75-in-pasco-county/

Food and Agriculture Sector

13. *December 14, U.S. Department of Agriculture* – (National) **USDA finalizes rule to enhance consumer protection, ensure retailers can track sources of ground meats.** The Food Safety and Inspection service announced December 14 that all makers of raw ground beef products will be required to keep adequate records of the source material, which include supplier lot numbers and production dates, dates and times of raw ground beef production, and dates and times of the cleaning and sanitization of grinding equipment and other related food-contact surfaces, among other requirements. The regulations align with expedited traceback and traceforward procedures announced in August 2014.
Source: http://www.fsis.usda.gov/wps/portal/fsis/newsroom/news-releases-statements-transcripts/news-release-archives-by-year/archive/2015/nr-121415-01

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

14. *December 14, Tampa Bay Times* – (International) **Man admits he smuggled $1.1 million in counterfeit male enhancement drugs like Viagra and Cialis from China.** Officials in Tampa charged the owner of Canadian American Drug Club and/or American Drug Club in Bradenton December 14 for allegedly making over $1.1 million from counterfeit prescription drugs imported from China. The man reportedly received shipments containing thousands of knockoff pills in order to fill unlicensed prescriptions through his business.
Source: http://home.tampabay.com/news/courts/criminal/man-admits-he-smuggled-11-million-in-counterfeit-male-enhancement-drugs/2257765

15. *December 14, WFTV 9 Orlando* – (Florida) **Man arrested, accused of running unlicensed medical clinic.** Officials with the Florida Division of Insurance Fraud announced December 14 that a man running an unlicensed clinic in Orange County was arrested and charged for allegedly committing tens of thousands of dollars' worth of insurance fraud. The man also hired medical doctors and chiropractors to pose as owners of the medical clinic to evade authorities.
Source: http://www.wftv.com/news/news/local/man-arrested-accused-running-unlicensed-medical-cl/npjsQ/

16. *December 14, Puget Sound Business Journal* – (Washington) **UW Medicine settles with feds over breach of data on 90,000 patients.** The U.S. Department of Health and Human Services announced December 14 that it reached a settlement with University of Washington Medicine resolving charges stemming from a November 2013 breach that potentially exposed the data of 90,000 patients after an employee downloaded a malicious email attachment. The medical school will pay $750,000 in penalties.
Source: http://www.bizjournals.com/seattle/blog/health-care-inc/2015/12/uw-medicine-settles-with-feds-over-breach-of-data.html

Government Facilities Sector

17. *December 15, KABC 7 Los Angeles* – (California) **San Bernardino Valley College closed Tuesday following bomb threat.** San Bernardino Valley College in California was closed December 15 after a bomb threat forced the evacuation of the campus December 14. The college will reopen once the campus is deemed safe following a search for any suspicious items.
Source: http://abc7.com/news/san-bernardino-valley-college-to-remain-closed-tuesday-following-bomb-threat/1122957/

18. *December 15, KTLA 5 Los Angeles* – (California) **LAUSD closes all schools amid 'credible threat' of violence to all schools: Officials.** School officials and police announced that all Los Angeles Unified School District schools were closed December 15 until further notice following a credible terror threat made towards the students mentioning explosive devices, assault rifles, and machine pistols. The district superintendent ordered a thorough search of all schools.
Source: http://ktla.com/2015/12/15/lausd-has-received-credible-terror-threat-district-

official-says/

19. *December 15, WOOD 8 Grand Rapids* – (Michigan) **Cedar Springs Public Schools closed due to power outage.** Crews worked to restore power following an outage that prompted the cancellation of all Cedar Springs Public Schools in Michigan December 15.
Source: http://woodtv.com/2015/12/15/cedar-springs-public-schools-closed-due-to-power-outage/

20. *December 14, KCPQ 13 Tacoma* – (Washington) **Substation fire near Bremerton knocks out power, forces several school closures.** Officials announced that Gateway Christian Schools, Green Mountain Elementary, and Kitsap Lake Elementary in Bremerton were closed December 14 following a substation fire that knocked out power to an unknown amount of customers.
Source: http://q13fox.com/2015/12/14/substation-fire-near-bremerton-knocks-out-power/

21. *December 14, WXIA 11 Atlanta* – (Georgia) **Report blames IT worker for voter data leak.** The Georgia Office of the Secretary of State released a report December 14 which determined that a former employee was to blame for the October 2015 leak of personal voter information to a dozen political and media organizations, and that the data leak began with a request from the State Department of Revenue for the personal information of more than 6 million State voters in August 2015.
Source: http://www.11alive.com/story/news/2015/12/14/voter-leak-report/77296308/

22. *December 14, U.S. Department of Justice* – (International) **U.S. Army National Guard soldier pleads guilty to attempting to provide material support to ISIL.** The U.S. Department of Justice announced that a U.S. Army National Guard soldier pleaded guilty December 14 to collaborating with a co-conspirator to provide material support to a designated foreign terrorist organization in the Middle East. The soldier also admitted to planning an attack at the National Guard base in Joliet, Illinois.
Source: https://www.fbi.gov/chicago/press-releases/2015/u.s.-army-national-guard-soldier-pleads-guilty-to-attempting-to-provide-material-support-to-isil

For another story, see item **4**

Emergency Services Sector

Nothing to report

Information Technology Sector

23. *December 15, Help Net Security* – (International) **13 million MacKeeper users exposed in data breach.** MacKeeper, the utility software for Apple Mac products, reported that its database containing passwords and the personal information of 13 million users were exposed in a data breach after a security researcher submitted a Shodan search and discovered four Internet Protocol (IP) addresses led to a MongoDB

database belonging to Kromtech, the company that produces MacKeeper. MacKeeper patched the vulnerability and reported no data was shared or used inappropriately.
Source: http://www.net-security.org/secworld.php?id=19232

24. *December 15, SecurityWeek* – (International) **Joomla patches zero-day exploited in the wild.** Joomla released its software version 3.4.6 and hotfixes patching a critical remote code execution flaw that was exploited in the wild for two days, enabling attackers to perform object injection via the Hypertext Transfer Protocol (HTTP) user agent which led to a full remote command execution attack from three different Internet Protocol (IP) addresses: 74.3.170.33, 146.0.72.83, and 194.28.174.106. The company advised users to check their logs for incoming requests from the three IP addresses and check if their Web sites were compromised by searching for "JDatabaseDriverMysqli" or "O:" in the User Agent.
Source: http://www.securityweek.com/joomla-patches-zero-day-exploited-wild

25. *December 15, Softpedia* – (International) **The return of macro malware and other malware trends.** Security researchers from Intel Security released a report stating there were two types of malicious campaigns using macro-based malware to compromise a user's personal computer (PC) via weaponized Word documents and another using fileless, in-memory malware to compromise a device by working in a PC's random-access memory (RAM). The report stated the office-based macro threats were the highest last seen within six years.
Source: http://news.softpedia.com/news/the-return-of-macro-malware-and-other-malware-trends-497590.shtml

26. *December 14, SecurityWeek* – (International) **Polycom patches flaw in VVX Business Media phones.** Polycom released software updates patching a path traversal vulnerability for several of its VVX Business Media phones after a security researcher from Depth Security found the request used by the interface displayed background images and ringtones in filename, which can allow attackers to use '../../' to back out of the ring tones and background image files and access sensitive file content using '/etc/passwd.' The company advised users to update its software to the latest version and disable the web servers on the affected devices.
Source: http://www.securityweek.com/polycom-patches-flaw-vvx-business-media-phones

For another story, see item **5**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

See item **26**

Commercial Facilities Sector

27. *December 14, Portland Oregonian* – (National) **West Linn police arrest six in interstate 'theft ring.'** The West Linn Police Department arrested 6 adults and 1 minor November 29 for alleged charges of first-degree aggravated theft, organized retail theft, aggravated identity theft, criminal possession of a forged instrument, and fraudulent use of a credit card after the suspects were linked to a theft ring scheme in which they victimized 110 people across 7 States by using stolen credit cards to buy more than $26,000 in gift cards.
Source: http://www.oregonlive.com/west-linn/index.ssf/2015/12/west_linn_police_arrest_six_in.html#incart_river_home

28. *December 14, USA Today* – (Oklahoma) **Video: disgruntled guest crashes pickup truck through Okla. hotel**. Oklahoma police arrested a Texas man December 14 for two felony counts of assault and battery with a dangerous weapon and one count of malicious injury to property after the man allegedly drove his truck through the front lobby of the Alva Comfort Inn and Suites, nearly hitting two employees due to a billing dispute with the hotel December 10. Building damages were estimated at more than $100,000.
Source: http://www.usatoday.com/story/news/2015/12/14/disgruntled-guest-crashes-hotel-truck/77333694/

29. *December 14, Freehold Patch* – (New Jersey) **Freehold movie theater set to reopen after bomb threat: Reports.** The AMC Freehold Metroplex at Freehold Raceway Mall in New Jersey was evacuated and closed for about two hours December 14 while police canine crews searched the building for explosive devices following a bomb threat. Authorities deemed the theater safe and found no explosive devices.
Source: http://patch.com/new-jersey/freehold/freehold-movie-theater-evacuated-police-ask-residents-avoid-area-0

30. *December 14, U.S. Department of Justice* – (Massachusetts) **Owners of Nick's Roast Beef charged with skimming nearly $6 million in cash.** The U.S. Department of Justice announced December 14 that the 2 owners of Nick's Famous Roast Beef in Beverly, and a co-conspirator were charged in connection to skimming nearly $6 million in cash receipts from the business from 2008 to 2013, and for failing to report the cash income on Federal tax returns. The trio allegedly stole over $1 million in cash receipts each year, created false cash register receipts to use during Internal Revenue Service audits, and failed to provide true cash register receipts to a tax preparer in order to avoid paying taxes.
Source: http://www.justice.gov/usao-ma/pr/owners-nick-s-roast-beef-charged-skimming-nearly-6-million-cash

Dams Sector

Nothing to report

U.S. DEPARTMENT OF HOMELAND SECURITY
NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.